

L'IA & Cybersécurité

L'Avenir de la Mobilité Automobile : Du Code à la Route



NEDEY.COM

Le Logiciel Devient Moteur

L'industrie automobile traverse un changement de paradigme fondamental. Nous passons d'une industrie "Hardware-defined" à l'ère du "Software-defined vehicle".

L'Intelligence Artificielle n'est plus une simple option d'aide à la conduite. Elle est le cœur du réacteur, conditionnant la compétitivité, la valeur et la sécurité des véhicules modernes.

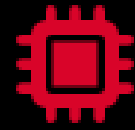


Les 3 Piliers de l'IA Embarquée



Conduite Autonome

Fusion de données multi-capteurs (Lidar, Radar, Vision) et réseaux de neurones pour une prise de décision en temps réel ultra-fiable.



Habitacle Intelligent

Création d'un cockpit digital immersif. Intégration de modèles LLM pour une personnalisation prédictive et un dialogue naturel.



Maintenance Prédictive

Analyse télémétrique continue. Anticipation des défaillances mécaniques et logicielles pour une approche "zéro panne".

L'Écosystème Informatique : **Edge vs Cloud**

Edge Computing (IA Locale)

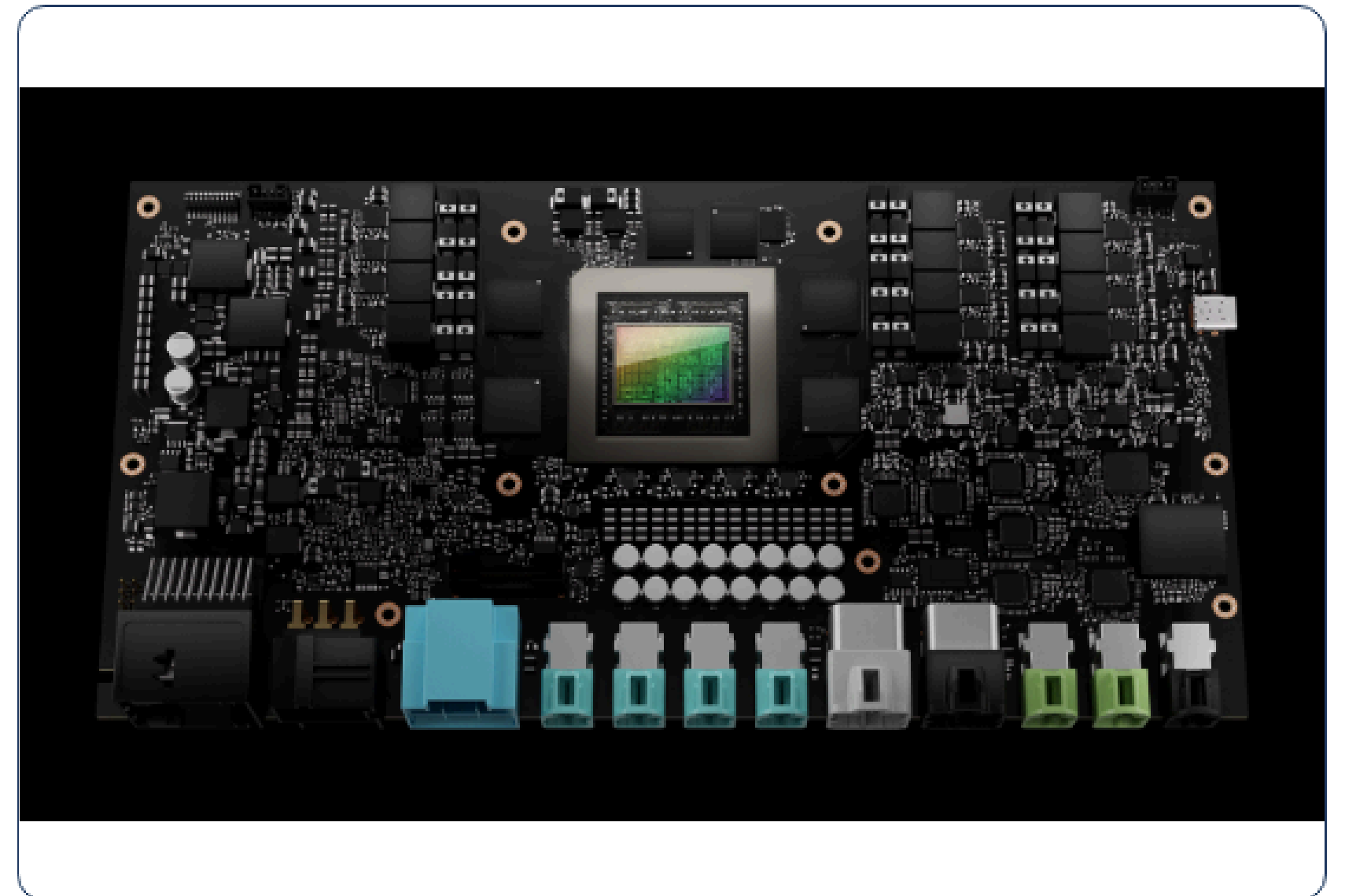
Le traitement des données critiques s'effectue directement **dans le véhicule**. C'est indispensable pour des décisions à **latence zéro** (ex: freinage d'urgence), le fonctionnement en "zone blanche" (sans réseau), et pour garantir la souveraineté des données de conduite privées.

Cloud Computing (Swarm Learning)

Le Cloud sert au "Machine Learning" de flotte. Les véhicules remontent des "edge cases" (scénarios rares) de manière anonymisée. Les algorithmes centraux sont réentraînés, puis redéployés sur l'ensemble du parc automobile via des mises à jour OTA.

L'Infrastructure Matérielle de l'IA

- ▶ **Processeurs Neuronaux (NPU) :** Pour exécuter l'IA embarquée, les CPU classiques ne suffisent plus. L'industrie intègre des SoC (System on Chip) spécialisés capables de traiter des téraoctets de données capteurs.
- ▶ **La Course aux TOPS :** La puissance se mesure en TOPS (Tera Operations Per Second). Les architectures modernes exigent plus de 500 TOPS pour atteindre la conduite autonome de niveau 3 ou
- ▶ **Efficacité Thermique :** Le défi informatique majeur est d'obtenir une puissance serveur dans un environnement soumis aux vibrations, aux températures extrêmes, tout en préservant la batterie (pour les VE).





Le Défi **Cybersécurité**

Protéger le "Super-Ordinateur sur roues" face à une surface d'attaque grandissante et professionnalisée.

Cartographie des Menaces

Attaques Réseaux & V2X

L'interconnexion globale expose le système au **Spoofing** (usurpation de signaux GPS/Capteurs pour tromper l'IA) et à l'interception ou la falsification de communications critiques entre le véhicule et l'infrastructure intelligente (feux, péages).

Compromission OS & Zero-Day

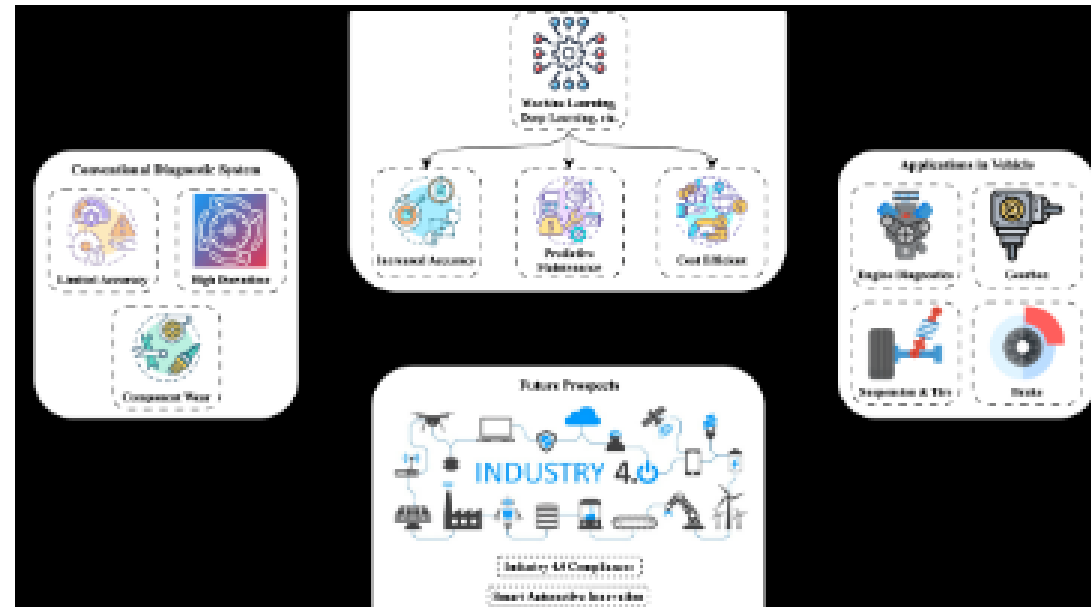
L'exploitation de failles non connues (Zero-day) dans l'OS embarqué peut mener à une **prise de contrôle à distance** des fonctions vitales (freinage par bus CAN) ou au lancement de Ransomware bloquant l'accès au véhicule.

Stratégie de Défense en Profondeur



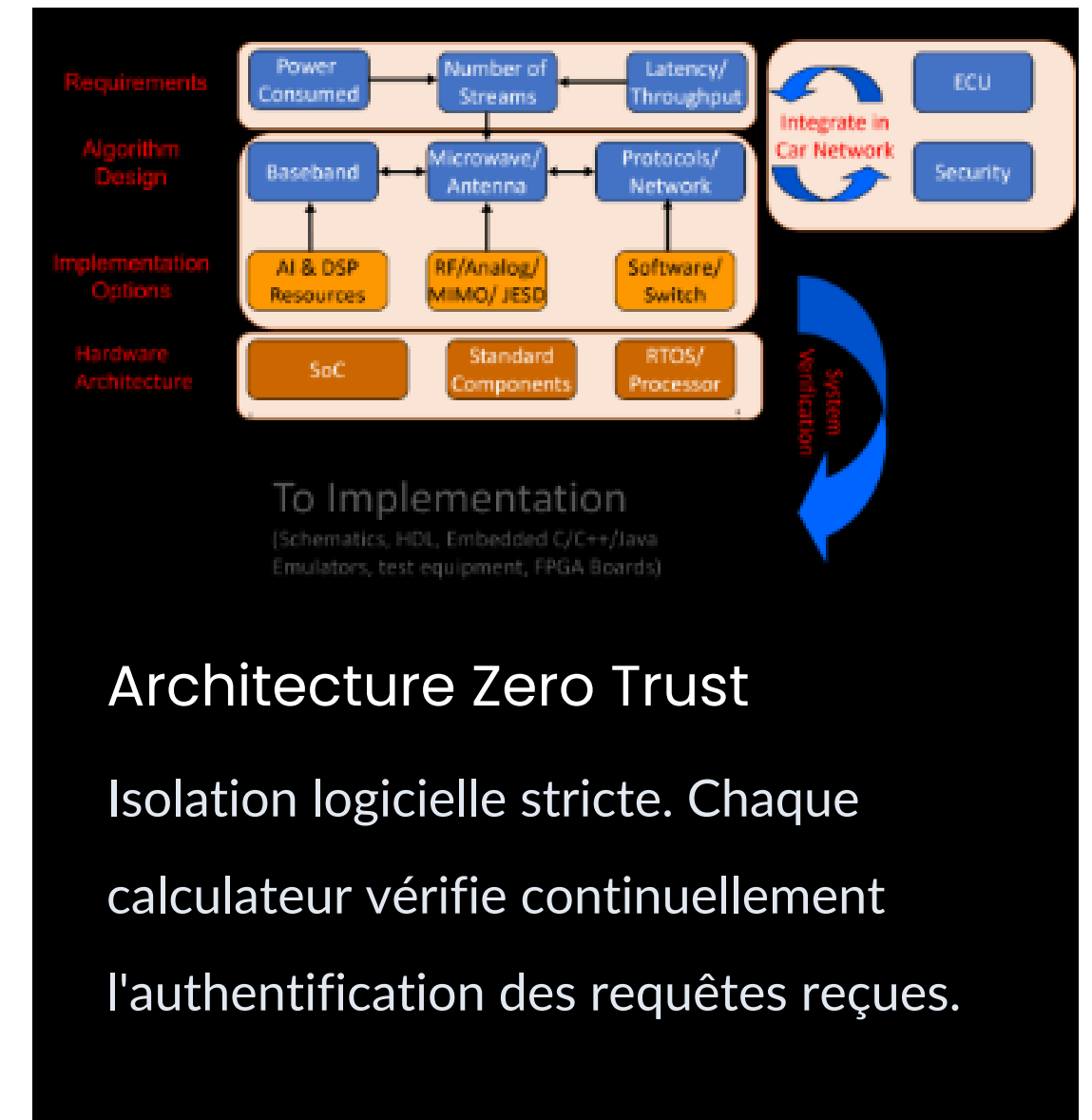
Chiffrement Hardened

Protection des clés cryptographiques dans des modules matériels sécurisés (HSM) intra-véhicule.



Détection par l'IA (IDS)

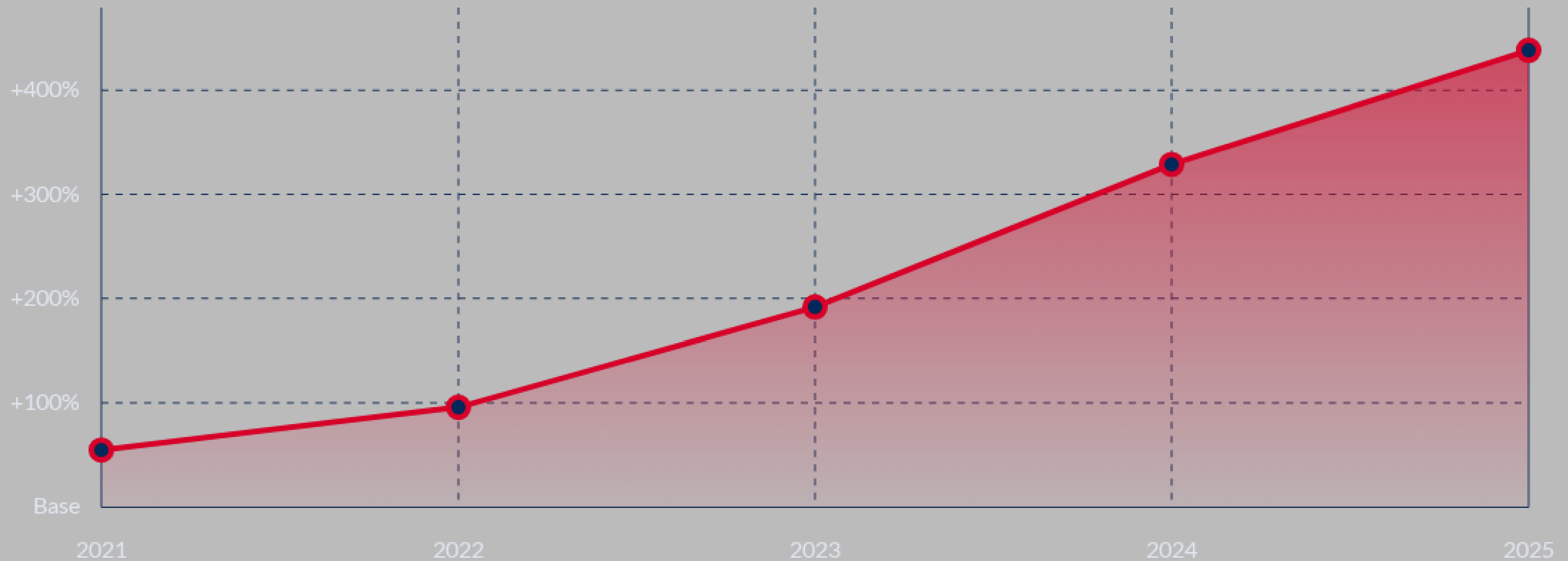
Machine Learning embarqué analysant le trafic réseau interne pour bloquer les injections de messages malveillants.



Architecture Zero Trust

Isolation logicielle stricte. Chaque calculateur vérifie continuellement l'authentification des requêtes reçues.

Explosion des **Cyberattaques** Automobiles



Croissance annuelle des incidents de sécurité cyber touchant l'écosystème automobile mondial.

Le Cadre **Réglementaire** Européen

Transformer la contrainte légale en avantage concurrentiel et en gage de confiance
absolue.

Homologation : **UNECE R155 & R156**

R155 : Le CSMS Obligatoire

Depuis juillet 2024 (Europe), les constructeurs doivent prouver qu'ils possèdent un **Cyber Security Management System (CSMS)**. Cela impose une cartographie et une gestion proactive des risques cyber tout au long du cycle de vie du véhicule, de la R&D jusqu'à la casse.

R156 : Le SUMS (Logiciel)

Le **Software Update Management System (SUMS)** régit les mises à jour OTA. La norme impose une traçabilité totale du code logiciel embarqué et oblige les marques à certifier qu'aucune mise à jour logicielle ne viendra corrompre la sécurité fonctionnelle du véhicule.

L'EU AI Act et la Protection des Données



L'IA à "Haut Risque"

L'Union Européenne classe les systèmes de conduite autonome (ADAS avancés) comme des systèmes d'IA à haut risque, imposant une documentation stricte et une surveillance humaine résiduelle.



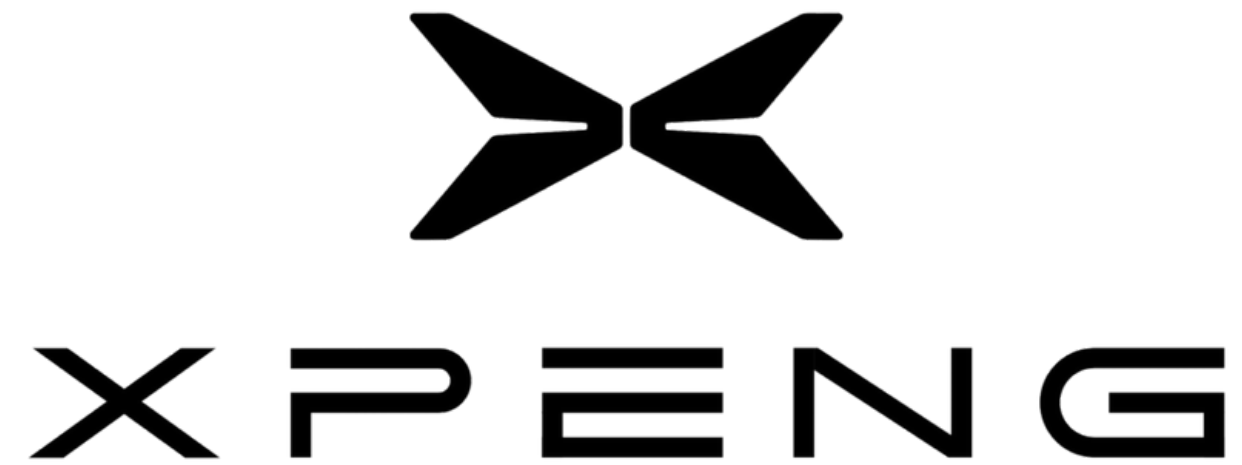
Audit & Explicabilité

Fini l'effet "Boîte Noire". Les algorithmes décisionnels devront être auditable en cas d'accident, nécessitant des architectures IA "explicables" et transparentes pour les autorités.



RGPD & Télémétrie

Un véhicule génère jusqu'à 25 Go de données par heure. L'anonymisation à la source (Edge) des données biométriques et vidéo devient une obligation légale pour le respect de la vie privée.



Le Cas Pratique **XPENG**

Comment l'IA et l'architecture matérielle redéfinissent l'expérience utilisateur et les standards d'un constructeur pionnier.

Architecture **SEPA 2.0** & XNGP

- ▶ **Architecture Centralisée** : SEPA 2.0 unifie le logiciel pour des mises à jour OTA fluides, gérant le véhicule entier comme un seul appareil ("Software as a Product").
- ▶ **Puissance de Calcul** : Puce Turing développant 750 TOPS
- ▶ **Système XNGP** : Navigation autonome de bout en bout urbaine, devenant indépendante de la cartographie haute définition grâce à l'IA prédictive.
- ▶ **Réseau XNet** : Réseaux neuronaux spatio-temporels pour la perception 3D dynamique continue.



Cockpit Digital : **XOS Tianji**



Le Copilote Digital Intégré

XPENG est précurseur en intégrant un grand modèle de langage (LLM) de manière native au sein du système d'exploitation du véhicule.

L'assistant "Xiao P" n'est plus une simple interface vocale. Il comprend le contexte spatial, visuel et audio, anticipe les besoins des passagers et gère de façon proactive les fonctions complexes du véhicule.

Merci de votre **attention**.

Les enjeux de l'IA et de la Cybersécurité redessinent notre industrie.

Place aux échanges et aux questions.

